

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the application:

LISTING OF CLAIMS:

1. (currently amended): A method for watermarking a document, comprising:
receiving said document;
generating an identification number based on said received document;
generating a seed based on said generated identification number;
~~associating said document with an identification number;~~
~~generating a first set of numbers using [[a]]the generated seed for said number~~
~~generation, comprising or derived from said identification number;~~
applying a transform to at least a portion of an image of said document to form a transform of said image;
defining a second set of numbers comprising transform coefficients from said transform of said image;
forming a modified second set of numbers based on said first set and said second set;
substituting said modified second set for said second set in said transform of said image to form a modified transform; and
applying an inverse of said transform to said modified transform to thereby produce a modified image of said document;
whereby said modified image of said document or an output of said modified image constitutes said watermarked document.

2. (original): A method as claimed in claim 1, including displaying, scanning or printing said watermarked version of said image of said document.

3. (original): A method as claimed in claim 1, including encrypting said identification number to produce an encrypted identification number, whereby said seed comprises said encrypted identification number.

4. (original): A method as claimed in claim 3, wherein said encrypting is by means of a one-way encryption function.

5. (original): A method as claimed in claim 4, wherein said first set of numbers have a Gaussian distribution with zero mean and unit variance.

6. (original): A method as claimed in claim 1, including applying said transform a plurality of times.

7. (original): A method as claimed in claim 1, including applying said transform a first time to produce a transformed image and applying said transform to at least a portion of said transformed image to form said transform of said image.

8. (original): A method as claimed in claim 1, wherein said transform is a wavelet transform.

9. (original): A method as claimed in claim 8, wherein said transform has a wavelet that is orthogonal, biorthogonal and symmetric.

10. (original): A method as claimed in claim 8, wherein said transform has a wavelet that is a Coiflets wavelet, a reverse biorthogonal wavelet, a biorthogonal wavelet, a Haar wavelet or a Daubechies wavelet.

11. (original): A method as claimed in claim 8, wherein said transform has a wavelet that is a Coiflets wavelet of order 4.

12. (original): A method as claimed in claim 1, wherein said transform coefficients correspond to middle frequency components of said transform.

13. (currently amended): A method as claimed in claim 8, wherein said transform coefficients are obtained from ~~the~~ a second level wavelet decomposition HH band of ~~the~~ a first level wavelet decomposition LL band.

14. (original): A method as claimed in claim 1, wherein said second set comprises a sequence of consecutive coefficients beginning at a predetermined starting point.

15. (original): A method as claimed in claim 1, wherein said second set comprises a sequence of consecutive coefficients beginning at a randomly selected starting point.

16. (original): A method as claimed in claim 1, including forming said modified second set of numbers based on a linear combination of said first set and said second set.

17. (currently amended): A method as claimed in claim 1, wherein, if said first set is represented by $A = \{a_1, a_2, \dots, a_n\}$ and said second set is represented by $B = \{b_1, b_2, \dots, b_n\}$, then said modified second set $B' = \{b'_1, b'_2, \dots, b'_n\} = B + \alpha \frac{|B|}{|A|} A$, wherein each $b'_x = b_x + \alpha \frac{|B|}{|A|} a_x$.

18. (original): A method as claimed in claim 17, including selecting α according to the nature of said document and a desired level of security.

19. (currently amended): A method as claimed in claim 1, including minimally modifying said second set when forming said modified second set such that said modified image can be validated on the basis of said seed after being printed and then digitized once, but such that said modified image cannot be validated on the basis of said seed if said modified image is subjected to ~~any~~ additional lossy processing.

20. (original): A method as claimed in claim 1, wherein said document is a passport, a passport photograph, an identity card, an identity card photograph or a certificate.

21. (currently amended): An apparatus for watermarking a document, comprising:
computing means operable to receive said document in digital form, to generate and an associated identification number based on said received document, to generate a seed based on said generated identification number, to generate a first set of numbers using ~~[[a]]~~ the generated seed for said number generation comprising or derived from said identification number, to apply a transform on at least a portion of an image of said document to generate a transform of said image, to define a second set of numbers comprising transform coefficients from said transform of said image of said document, to form a modified second set of numbers based on said first set and said second set, to substitute said modified second set for said second set in said transform of said image to form a modified transform, and to apply an inverse of said transform to said modified transform to thereby produce a modified image of said document; and

output means to provide an output of said modified image of said document; wherein said output constitutes said watermarked document.

22. (currently amended): An apparatus as claimed in claim 21, including a scanner for converting said document in hardcopy form into said digital form and transmitting the document in digital form to said computing means, said scanner being in electronic communication with said computing means.

23. (currently amended): An apparatus as claimed in claim 21, wherein said computing means is operable to encrypt said identification number to produce an encrypted identification number, whereby said seed comprises said encrypted identification number. ~~More preferably,~~ wherein said computing means is operable to encrypt said identification number by means of a one-way encryption function.

24. (original): An apparatus as claimed in claim 21, wherein said transform is a wavelet transform.

25. (original): An apparatus as claimed in claim 24, wherein said computing means is operable to perform said transform with a wavelet that is a Coiflets wavelet of order 4.

26. (currently amended): An apparatus as claimed in claim 24, wherein said transform coefficients are obtained from ~~the~~ a second level wavelet decomposition HH band of ~~the~~ a first level wavelet decomposition LL band.

27. (currently amended): An apparatus as claimed in claim 21, wherein said computing means is operable to form said modified second set of numbers based on a linear combination of said first set and said second set. ~~More preferably,~~ wherein if said first set is represented by $A = \{a_1, a_2, \dots, a_n\}$ and said second set is represented by $B = \{b_1, b_2, \dots, b_n\}$, then said modified second set $B' = \{b'_1, b'_2, \dots, b'_n\} = B + \alpha/B/A \ B + \alpha|B|A$, wherein each $b'_x = b_x + \alpha/b_x/a_x \ b_x + \alpha|b_x|a_x$.

28. (currently amended): An apparatus as claimed in claim 21, wherein said computing means is operable to minimally modify said second set when forming said modified second set such that said modified image can be validated on the basis of said seed after being printed and

then digitized once, but such that said modified image cannot be validated on the basis of said seed if said modified image is subjected to ~~any~~ additional lossy processing.

29. (currently amended): A method of checking ~~the~~ a validity of ~~[[a]]an input~~ document watermarked according to the method of claim 1, the method comprising:

generating a first set of numbers using a seed for said number generation comprising or derived from an ~~associated~~ identification number of the watermarked document, wherein the identification number is generated based on the input watermarked document;

applying a transform to at least a portion of ~~[[an]]a~~ watermarked image of said watermarked document to generate a transform of said watermarked image;

defining a second set of numbers comprising transform coefficients from said transform of said watermarked image of said watermarked document; and

determining ~~what a~~ level of correlation ~~exists~~ between said first and second sets of numbers;

wherein said document is validated according to said level of the correlation.

30. (currently amended): A method as claimed in claim 1, wherein said generating said first set of numbers comprises randomly generating said first set of numbers based on the generated seed.

31. (original): A method of checking the validity of a document watermarked according to the method of claim 29, including transmitting said document over a computer network to a verification system for checking, and receiving a result of said checking over said computer network from said verification system.

32. (currently amended): An apparatus for checking ~~the~~ a validity of ~~[[a]]an input~~ document watermarked according to the method of claim 21, comprising:

~~computing~~ means operable to generate a first set of numbers using a seed for said number generation comprising or derived from an ~~associated~~ identification number of the input watermarked document, wherein the identification number is generated based on the input watermarked document, to apply a transform on at least a portion of ~~[[an]]~~ a watermarked image of said watermarked document to generate a transform of said watermarked image, to define a second set of numbers comprising transform coefficients from said transform of said watermarked image of said watermarked document; and

means for determining what a level of correlation exists between said first and second sets of numbers;

wherein said document can be validated according to said level of the correlation.

33. (currently amended): A method of checking the validity of a document. over a computer network, comprising:

a user electronically submitting a document that has been provided with a watermark according to the method of claim 1, or a copy of said document, via said computer network to a verification system;

said verification system electronically checking the validity of said document according to said ~~[[the]]~~ watermark and legible identification information appearing on said document; and

said verification system electronically transmitting to said user or a nominated alternative user a result of said checking of said validity.

34. (original): A method as claimed in claim 33, wherein said legible identification information comprises or includes a name of a person to whom said document pertains.

35. (original): A method as claimed in claim 33, further including said user inputting said legible identification information.

36. (original): A method as claimed in claim 33, further including said verification system employing character recognition and thereby extracting said legible identification information from said document.

37. (currently amended): A method as claimed in claim 33, wherein said document comprises a certification of academic attainment and said legible identification information comprises ~~or includes~~ any one or more of: ~~the~~ a name of ~~the~~ a holder of said academic attainment and ~~the~~ a name of said academic attainment.

38. (original): A method as claimed in claim 33, wherein said computer network comprises the internet or an intranet.

39. (currently amended): An apparatus for providing a digital image with a digital watermark, comprising:

computing means operable a) to receive said digital image, ~~and~~ to generate an associated identification number based on said received digital image, and to generate a seed based on said generated identification number, b) to generate a first set of numbers using ~~[[a]]~~ the generated seed for said number generation comprising or derived from said identification number, c) to apply a transform on at least a portion of said digital image to generate a transform of said digital image, transform coefficients from said transform constituting a second set of numbers, d) to form a modified second set of numbers based on said first set and said second set, e) to substitute said modified second set for said second set in said transform of said digital image to form a modified transform, and f) to apply an inverse of said transform to said modified transform to thereby produce a modified digital image: and

output means to output said modified digital image.